特 許 協 力 条 約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第12条、法施行規則第56条）
〔ＰＣＴ36条及びＰＣＴ規則70〕

出願人又は代理人の書類記号 MA-620-PCT	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ２００５／００１１７７	国際出願日 （日．月．年） ２１．０１．２００５	優先日 （日．月．年） ２３．０１．２００４
国際特許分類（ＩＰＣ） Int.Cl. *H04L9/32 (2006.01), G09C1/00 (2006.01)*		
出願人（氏名又は名称） 日本電気株式会社		

１．この報告書は、ＰＣＴ35条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ36条）の規定に従い送付する。

２．この国際予備審査報告は、この表紙を含めて全部で 3 ページからなる。

３．この報告には次の附属物件も添付されている。

ａ．☐ 附属書類は全部で＿＿＿＿＿＿ ページである。

☐ 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第607号参照）

☐ 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

ｂ．☐ 電子媒体は全部で＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、電子形式による配列表又は配列表に関連するテーブルを含む。
（実施細則第802号参照）

４．この国際予備審査報告は、次の内容を含む。

☑ 第Ｉ欄 国際予備審査報告の基礎
☐ 第Ⅱ欄 優先権
☐ 第Ⅲ欄 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
☐ 第Ⅳ欄 発明の単一性の欠如
☑ 第Ⅴ欄 ＰＣＴ35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
☐ 第Ⅵ欄 ある種の引用文献
☐ 第Ⅶ欄 国際出願の不備
☐ 第Ⅷ欄 国際出願に対する意見

国際予備審査の請求書を受理した日 ２４．１１．２００５	国際予備審査報告を作成した日 １２．０１．２００６
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） ５Ｓ ４２２９ 青木 重徳 電話番号 ０３－３５８１－１１０１ 内線 ３５４６

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００５年４月）

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００１１７７

第Ⅰ欄　報告の基礎

1．言語に関し、この予備審査報告は以下のものを基礎とした。

☑ 出願時の言語による国際出願

☐ 出願時の言語から次の目的のための言語である＿＿＿＿＿＿ 語に翻訳された、この国際出願の翻訳文

- ☐ 国際調査（ＰＣＴ規則12.3(a)及び23.1(b)）
- ☐ 国際公開（ＰＣＴ規則12.4(a)）
- ☐ 国際予備審査（ＰＣＴ規則55.2(a)又は55.3(a)）

2．この報告は下記の出願書類を基礎とした。（法第6条（ＰＣＴ14条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☑ 出願時の国際出願書類

☐ 明細書

第＿＿＿＿＿＿＿＿ ページ、出願時に提出されたもの
第＿＿＿＿＿＿＿＿ ページ*、＿＿＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの
第＿＿＿＿＿＿＿＿ ページ*、＿＿＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 請求の範囲

第＿＿＿＿＿＿＿＿ 項、出願時に提出されたもの
第＿＿＿＿＿＿＿＿ 項*、ＰＣＴ１９条の規定に基づき補正されたもの
第＿＿＿＿＿＿＿＿ 項*、＿＿＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの
第＿＿＿＿＿＿＿＿ 項*、＿＿＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 図面

第＿＿＿＿＿＿＿＿ ページ／図 、出願時に提出されたもの
第＿＿＿＿＿＿＿＿ ページ／図 *、＿＿＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの
第＿＿＿＿＿＿＿＿ ページ／図 *、＿＿＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

3．☐ 補正により、下記の書類が削除された。

- ☐ 明細書　第＿＿＿＿＿＿＿＿ ページ
- ☐ 請求の範囲　第＿＿＿＿＿＿＿＿ 項
- ☐ 図面　第＿＿＿＿＿＿＿＿ ページ／図
- ☐ 配列表（具体的に記載すること）＿＿＿＿＿＿＿＿
- ☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿＿＿

4．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)）

- ☐ 明細書　第＿＿＿＿＿＿＿＿ ページ
- ☐ 請求の範囲　第＿＿＿＿＿＿＿＿ 項
- ☐ 図面　第＿＿＿＿＿＿＿＿ ページ／図
- ☐ 配列表（具体的に記載すること）＿＿＿＿＿＿＿＿
- ☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿＿＿

＊ 4．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号 ＰＣＴ／ＪＰ２００５／００１１７７

第Ⅴ欄　新規性、進歩性又は産業上の利用可能性についての法第12条（ＰＣＴ35条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（Ｎ）	請求の範囲	１－１２	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲		有
	請求の範囲	１－１２	無
産業上の利用可能性（ＩＡ）	請求の範囲	１－１２	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

文献１：Kazue Umeda, Atsuko Miyaji, “A Group Signatue based on Nyberg-Ryeppel Signatures”, ２００３年暗号と情報セキュリティシンポジウム予稿集, Volume 1 of 2, 2003.01.26, ｐ．３２７－３３２

文献２：加藤隆充, 廣瀬勝一, 三輪導彦, 池田克夫, “Elgamal の公開鍵暗号系に基づくグループ署名による署名プロトコル”, １９９２年電子情報通信学会－創立７５周年記念－秋季大会講演論文集, 分冊１, 1992.08.15, ｐ．１・１８７

請求の範囲１－１２に係る発明は、国際調査報告で引用された文献１と文献２とにより進歩性を有しない。

文献１には、Nyberg-Rueppel 署名を用いたグループ署名技術が記載されており、離散対数問題に基づく暗号系からメンバー追跡や署名者追跡に用いる秘密情報を生成して分散管理を行うことで管理者権限の分散を行うことが記載されている。

文献２には、秘密鍵を Shamir の閾値方式で複数のデータに変換して分割管理し、署名作成の際は分割管理されている前記秘密鍵を復元することなくグループ署名を行い、一方でグループメンバーのうちｎ人が協力することで前記秘密鍵の復元を可能とする離散対数問題に基づく暗号系を用いたグループ署名プロトコルが記載されている。

そして、文献１，２が共に離散対数問題に基づく暗号系を用いたグループ署名技術について記載したものである点を勘案すれば、文献１に記載されているグループ署名技術における管理者権限の分散として、文献２に記載されているものを採用し、署名作成時には Shamir の閾値方式で分割管理している秘密鍵を復元することなく Nyberg-Rueppel 署名を用いたグループ署名を行えるようにし、署名者追跡を行う必要がある場合にはグループメンバーのうちｎ人が協力すること前記秘密鍵を復元することで追跡が行えるようにした方法を想到し、システム構成することは、当業者にとって容易であるし、このように秘密鍵が複数のデータに分割変換されているので管理者によるグループ署名データの偽造が困難であることは当業者にとって自明である。